

CIP 11.0430

Exam 70-290

## **Managing and Maintaining a Microsoft Windows Server 2003 Environment**

### **Audience Profile**

The Microsoft Certified Systems Administrator (MCSA) on Windows Server 2003 credential is intended for IT professionals who work in the typically complex computing environment of medium to large companies. An MCSA candidate should have 6 to 12 months of experience administering client and network operating systems in environments that have the following characteristics:

- 250 to 5,000 or more users
- Three or more physical locations
- Three or more domain controllers
- Network services and resources such as messaging, database, file and print, proxy server, firewall, Internet, intranet, remote access, and client computer management
- Connectivity requirements such as connecting branch offices and individual users in remote locations to the corporate network and connecting corporate networks to the Internet

### **Skills Being Measured**

This exam measures your ability to accomplish the technical tasks listed below. The percentages indicate the relative weight of each major topic area on the exam.

#### **01 Managing and Maintaining Physical and Logical Devices**

- Manage basic disks and dynamic disks.
- Monitor server hardware. Tools might include Device Manager, the Hardware Troubleshooting Wizard, and appropriate Control Panel items.
- Optimize server disk performance.
  - Implement a RAID solution.
  - Defragment volumes and partitions.
- Troubleshoot server hardware devices.
  - Diagnose and resolve issues related to hardware settings.
  - Diagnose and resolve issues related to server hardware and hardware driver upgrades.
- Install and configure server hardware devices.
  - Configure driver signing options.
  - Configure resource settings for a device.
  - Configure device properties and settings.

#### **02 Managing Users, Computers, and Groups**

- Manage local, roaming, and mandatory user profiles.
- Create and manage computer accounts in an Active Directory environment.
- Create and manage groups.
  - Identify and modify the scope of a group.
  - Find domain groups in which a user is a member.
  - Manage group membership.
  - Create and modify groups by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.
  - Create and modify groups by using automation.
- Create and manage user accounts.
  - Create and modify user accounts by using the Active Directory Users and Computers MMC snap-in.
  - Create and modify user accounts by using automation.

- Import user accounts.
- Troubleshoot computer accounts.
  - Diagnose and resolve issues related to computer accounts by using the Active Directory Users and Computers MMC snap-in.
  - Reset computer accounts.
- Troubleshoot user authentication issues.

### **03 Managing and Maintaining Access to Resources**

- Configure access to shared folders.
  - Manage shared folder permissions.
- Troubleshoot Terminal Services.
  - Diagnose and resolve issues related to Terminal Services security.
  - Diagnose and resolve issues related to client access to Terminal Services.
- Configure file system permissions.
  - Verify effective permissions when granting permissions.
  - Change ownership of files and folders.
- Troubleshoot access to files and shared folders.

### **04 Managing and Maintaining a Server Environment**

- Monitor and analyze events. Tools might include Event Viewer and System Monitor.
- Manage software update infrastructure.
- Manage software site licensing.
- Manage servers remotely.
  - Manage a server by using Remote Assistance.
  - Manage a server by using Terminal Services remote administration mode.
  - Manage a server by using available support tools.
- Troubleshoot print queues.
- Monitor system performance.
- Monitor file and print servers. Tools might include Task Manager, Event Viewer, and System Monitor.
  - Monitor disk quotas.
  - Monitor print queues.
  - Monitor server hardware for bottlenecks.
- Monitor and optimize a server environment for application performance.
  - Monitor memory performance objects.
  - Monitor network performance objects.
  - Monitor process performance objects.
  - Monitor disk performance objects.
- Manage a Web server.
  - Manage Internet Information Services (IIS).
  - Manage security for IIS.

### **05 Managing and Implementing Disaster Recovery**

- Perform system recovery for a server.
  - Implement Automated System Recovery (ASR).
  - Restore data from shadow copy volumes.
  - Back up files and System State data to media.
  - Configure security for backup operations.
- Manage backup procedures.
  - Verify the successful completion of backup jobs.

- Manage backup storage media.
- Recover from server hardware failure.
- Restore backup data.
- Schedule backup jobs.